Broadvoice Leak Exposes 350M Records, Personal Voicemail Transcripts

By Tara Seals

Published: 2020-10-15 · Archived: 2026-04-05 23:00:32 UTC

Companies that use Broadvoice's cloud-based VoIP platform may find their patients, customers, suppliers and partners to be impacted by a massive data exposure.

UPDATE

Broadvoice, a well-known VoIP provider that serves small- and medium-sized businesses, has leaked more than 350 million customer records related to the company's "b-hive" cloud-based communications suite.

The data includes hundreds of thousands of voicemail transcripts, many involving sensitive information such as details about medical prescriptions and financial loans.

Broadvoice provides one of the more popular business platforms for communications, which includes voice, contact-center technology, remote-workforce help, Salesforce.com integration, unified communications, SIP trunking and more. Much of this is offered via b-hive, which it hosts on behalf of customers such as doctors' offices, law firms, retail stores, community organizations and more.

Because its technology underpins these customers' basic interactions with patients, clients, partners, suppliers and others, plenty of personal data flows through Broadvoice's cloud-based systems. And that data is apparently retained by the company, so that its business clients can access it if needed, for analytics and call-center quality control, among other things.

Unfortunately, according to researchers at Comparitech, Broadvoice left an Elasticsearch database cluster containing such information open to the internet, accessible to anyone, with no authentication required. The cache of data included records with personal details of Broadvoice clients' customers, they noted.

The misconfigured cluster included 10 separate collections of data, related to b-hive.

The largest collection (275 million records) included full caller name, caller ID, phone number, and city and state. Meanwhile, a collection entitled "people-production" contained account ID numbers for Broadvoice's own customers, which allowed researchers to cross-reference entries with records in other collections.

But the most concerning one held 2 million voicemail records, with more than 200,000 transcripts.

“Many of the transcripts included select personal details such as full name, phone number and date of birth, as well as some sensitive information,” according to a Comparitech posting on Thursday. “For example, some transcripts of voicemails left at medical clinics included names of prescriptions or details about medical procedures. In one transcript, the caller identified themselves by their full name and discussed a positive COVID-19 diagnosis.”

Researchers added, “Other voicemails left for financial-service companies included details about mortgages and other loans, while there was at least one instance of an insurance-policy number being disclosed.”

Most of these records also contained a full name, business name or a generic name such as “wireless caller”; phone number; a name or identifier for the voice mailbox (such as “appointments”); and internal identifiers, according to Comparitech.

When reached for comment about Broadvoice’s data-retention policies, and whether its business customers will be issuing data-breach notifications to their own affected customers, Rebecca Rosen, vice president of marketing, told Threatpost that the number of impacted businesses is likely less than 10,000.

“To provide some perspective, we believe that the researcher accessed a sub-set of data that potentially impacted less than 10,000 customers,” she said. “Our investigation is otherwise ongoing, and we are not otherwise commenting or speculating other than what we have posted online.”

Aside from the privacy implications, the data paves the way for convincing fraud attempts, researchers noted.

“The leaked database represents a wealth of information that could help facilitate targeted phishing attacks,” according to Comparitech. “In the hands of fraudsters, it would offer a ripe opportunity to dupe Broadvoice clients and their customers out of additional information and possibly into handing over money. For example, criminals could pose as Broadvoice or one of its clients to convince customers to provide things like account login credentials or financial information.”

Meanwhile, “information about things like medical prescriptions and loan enquiries could be used to make messages extremely convincing and persuasive.”

The collections were discovered by researcher Bob Diachenko on Oct. 1, and were secured the same day, according to Broadvoice. The cluster had been uploaded on Sept. 28, meaning it was exposed for about four days.

“Broadvoice takes data privacy and security seriously,” Broadvoice CEO Jim Murphy said in a statement. He added, “At this point, we have no reason to believe that there has been any misuse of the data. We are currently

engaging a third-party forensics firm to analyze this data and will provide more information and updates to our customers and partners. We cannot speculate further about this issue at this time."

He also said that Broadvoice is working with Diachenko to ensure that the retained data is destroyed.

This story was updated at 1 p.m. ET on Oct. 15 to include a statement from Broadvoice's vice president of marketing.
